Router Cisco IOS: Esempio di autenticazione locale, TACACS+ e RADIUS della configurazione della connessione HTTP

Sommario

Introduzione

In questo documento viene spiegato come configurare l'autenticazione locale, TACACS+ e RADIUS della connessione HTTP. Vengono inoltre forniti alcuni comandi di debug rilevanti.

Operazioni preliminari

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Prerequisiti

Non sono previsti prerequisiti specifici per questo documento.

Componenti usati

Le informazioni fornite in questo documento si basano sulle versioni software e hardware riportate

di seguito.

- Software Cisco IOS® versione 11.2 o successive
- Hardware che supporta queste revisioni software

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Nozioni di base

Nel software Cisco IOS® versione 11.2, è stata aggiunta una funzionalità per gestire il router tramite HTTP. La sezione "Comandi del browser Web Cisco IOS" della guida di riferimento dei comandi di Cisco IOS Configuration Fundamentals include le seguenti informazioni su questa funzione.

"Il comando **ip http authentication** consente di specificare un particolare metodo di autenticazione per gli utenti del server HTTP. Il server HTTP utilizza il metodo enable password per autenticare un utente con livello di privilegio 15. Il comando **ip http authentication** consente ora di specificare l'autenticazione dell'utente del server HTTP enable, local, TACACS o authentication, authorization, and accounting (AAA)."

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Questo documento utilizza le configurazioni mostrate di seguito.

- Configurazione dell'autenticazione locale per gli utenti del server HTTP
- Configurazione dell'autenticazione TACACS+ per gli utenti del server HTTP
- Configurazione dell'autenticazione RADIUS per gli utenti del server HTTP

Nota: per ulteriori informazioni sui comandi menzionati in questo documento, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Configurazione dell'autenticazione locale per gli utenti del server HTTP

- Configurazioni router
- Risultati utente

Configurazioni router

Autenticazione locale con software Cisco IOS versione 11.2
`!--- This is the part of the configuration related to local authentication. ! aaa new-model aaa authentication login default local aaa authorization exec local username one privilege 15 password one username three`

```
password three username four privilege 7 password four
ip http server ip http authentication aaa ! !--- Example
of command moved from level 15 (enable) to level 7 !
privilege exec level 7 clear line
```

Autenticazione locale con software Cisco IOS versione 11.3.3.T o successive

```
!--- This is the part of the configuration !--- related
to local authentication. ! aaa new-model aaa
authentication login default local aaa authorization
exec default local username one privilege 15 password
one username three password three username four
privilege 7 password four ip http server ip http
authentication local ! !--- Example of command moved
from level 15 (enable) to level 7 ! privilege exec level
7 clear line
```

Risultati utente

i risultati si applicano agli utenti nelle precedenti configurazioni del router.

- **Utente uno**L'utente passerà l'autorizzazione Web se l'URL viene immesso come http://#.#.#.#.Dopo aver eseguito Telnet sul router, l'utente può eseguire tutti i comandi dopo l'autenticazione di accesso.L'utente sarà in modalità abilitazione dopo l'accesso (il **privilegio show** sarà 15).Se l'autorizzazione del comando viene aggiunta al router, l'utente avrà comunque esito positivo in tutti i comandi.
- **Utente tre**L'utente non riuscirà a ottenere l'autorizzazione Web perché non dispone di un livello di privilegio.Dopo aver eseguito Telnet sul router, l'utente può eseguire tutti i comandi dopo l'autenticazione di accesso.L'utente sarà in modalità non abilitazione dopo l'accesso (il **privilegio show** sarà 1).Se l'autorizzazione del comando viene aggiunta al router, l'utente avrà comunque esito positivo in tutti i comandi.
- **Utente quattro**L'utente passerà l'autorizzazione Web se l'URL viene immesso come http://#.#.#.#/level/7/exec.Verranno visualizzati i comandi di livello 1 più il comando **clear line di** livello 7.Dopo aver eseguito Telnet sul router, l'utente può eseguire tutti i comandi dopo l'autenticazione di accesso.L'utente sarà al livello di privilegio 7 dopo l'accesso (**il privilegio show** sarà 7)Se l'autorizzazione del comando viene aggiunta al router, l'utente avrà comunque esito positivo in tutti i comandi.

Configurazione dell'autenticazione TACACS+ per gli utenti del server HTTP

Configurazioni router

Autenticazione con il software Cisco IOS versione 11.2

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Autenticazione con software Cisco IOS versioni da 11.3.3.T a 12.0.5.T

```
aaa new-model
aaa authentication login default tacacs+
aaa authorization exec default tacacs
ip http server
ip http authentication aaa|tacacs
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Autenticazione con il software Cisco IOS versione 12.0.5.T e successive

```
aaa new-model
aaa authentication login default group tacacs+
aaa authorization exec default group tacacs+
ip http server
ip http authentication aaa
tacacs-server host 171.68.118.101
tacacs-server key cisco
!--- Example of command moved from level 15 (enable) to
level 7 privilege exec level 7 clear line
```

Risultati utente

I risultati seguenti si applicano agli utenti nelle configurazioni server riportate di seguito.

- **Utente uno**L'utente passerà l'autorizzazione Web se l'URL viene immesso come http://#.#.#.#.Dopo aver eseguito Telnet sul router, l'utente può eseguire tutti i comandi dopo l'autenticazione di accesso.L'utente sarà in modalità abilitazione dopo l'accesso (il **privilegio show** sarà 15).Se l'autorizzazione del comando viene aggiunta al router, l'utente avrà comunque esito positivo in tutti i comandi.
- **Utente due**L'utente passerà l'autorizzazione Web se l'URL viene immesso come http://#.#.#.#.Dopo aver eseguito Telnet sul router, l'utente può eseguire tutti i comandi dopo l'autenticazione di accesso.L'utente sarà in modalità abilitazione dopo l'accesso (il **privilegio show** sarà 15).Se si aggiunge l'autorizzazione del comando al router, l'utente non riuscirà a eseguire tutti i comandi perché la configurazione del server non li autorizza.
- **Utente tre**L'utente non riuscirà a ottenere l'autorizzazione Web perché non dispone di un livello di privilegio.Dopo aver eseguito Telnet sul router, l'utente può eseguire tutti i comandi dopo l'autenticazione di accesso.L'utente sarà in modalità non abilitazione dopo l'accesso (il **privilegio show** sarà 1).Se l'autorizzazione del comando viene aggiunta al router, l'utente avrà comunque esito positivo in tutti i comandi.

- **Utente quattro**L'utente passerà l'autorizzazione Web se l'URL viene immesso come http://#.#.#.#/level/7/exec.Verranno visualizzati i comandi di livello 1 più il comando **clear line di** livello 7.Dopo aver eseguito Telnet sul router, l'utente può eseguire tutti i comandi dopo l'autenticazione di accesso.L'utente sarà al livello di privilegio 7 dopo l'accesso (**il privilegio show** sarà 7)Se l'autorizzazione del comando viene aggiunta al router, l'utente avrà comunque esito positivo in tutti i comandi.

Configurazione server del daemon di freeware

```
user = one {
default service = permit
login = cleartext "one"
service = exec {
priv-lvl = 15
}
}

user = two {
login = cleartext "two"
service = exec {
priv-lvl = 15
}
}

user = three {
default service = permit
login = cleartext "three"
}

user = four {
default service = permit
login = cleartext "four"
service = exec {
priv-lvl = 7
}
}
```

Configurazione server Cisco Secure ACS per UNIX

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 27
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=15
}
}
# ./ViewProfile -p 9900 -u two
User Profile Information
user = two{
profile_id = 28
profile_cycle = 1
password = clear "********"
service=shell {
set priv-lvl=15
```

```
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 29
profile_cycle = 1
password = clear "********"
default service=permit
}
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 30
profile_cycle = 1
password = clear "********"
default service=permit
service=shell {
set priv-lvl=7
}
}
```

[Configurazione Cisco Secure ACS per Windows Server]

Utente uno nel gruppo uno

- Impostazioni gruppoControllare la **shell (exec)**.Selezionare **Privilege Level=15**.Selezionare **Servizi predefiniti (non definiti)**.**Nota:** se questa opzione non viene visualizzata, andare a **Configurazione interfaccia** e selezionare **TACACS+**, quindi **Opzioni di configurazione avanzate**. Scegliere **Visualizza** configurazione **predefinita (non definita)**.
- Impostazioni utentePassword da qualsiasi database; immettere la password e confermare nell'area superiore.

Utente due nel gruppo due

- Impostazioni gruppoControllare la **shell (exec)**.Selezionare **Privilege Level=15**.Non selezionare **Servizi predefiniti (non definiti)**.
- Impostazioni utentePassword da qualsiasi database; immettere la password e confermare nell'area superiore.

Utente tre nel gruppo tre

- Impostazioni gruppoControllare la **shell (exec)**.Lasciare vuoto **il livello di privilegio**.Selezionare **Servizi predefiniti (non definiti)**.**Nota:** se questa opzione non viene visualizzata, andare a **Configurazione interfaccia** e selezionare **TACACS+**, quindi **Opzioni di configurazione avanzate**. Scegliere **Visualizza** configurazione **predefinita (non definita)**.
- Impostazioni utentePassword da qualsiasi database; immettere la password e confermare nell'area superiore.

Utente quattro nel gruppo quattro

- Impostazioni gruppoControllare la **shell (exec)**.Selezionare **Privilege Level=7**.Selezionare **Servizi predefiniti (non definiti)**.**Nota:** se questa opzione non viene visualizzata, andare a **Configurazione interfaccia** e selezionare **TACACS+**, quindi **Opzioni di configurazione avanzate**. Scegliere **Visualizza** configurazione **predefinita (non definita)**.
- Impostazioni utentePassword da qualsiasi database; immettere la password e confermare nell'area superiore.

Configurazione dell'autenticazione RADIUS per gli utenti del server HTTP

Configurazioni router

Autenticazione con il software Cisco IOS versione 11.2

```
aaa new-model
aaa authentication login default radius
aaa authorization exec radius
ip http server
ip http authentication aaa
!
!--- Example of command moved from level 15 (enable) to
level 7 ! privilege exec level 7 clear line radius-
server host 171.68.118.101 radius-server key cisco
```

Autenticazione con software Cisco IOS versioni da 11.3.3.T a 12.0.5.T

```
aaa new-model
aaa authentication login default radius
aaa authorization exec default radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Autenticazione con il software Cisco IOS versione 12.0.5.T e successive

```
aaa new-model
aaa authentication login default group radius
aaa authorization exec default group radius
ip http server
ip http authentication aaa
radius-server host 171.68.118.101 auth-port 1645 acct-
port 1646
radius-server key cisco
privilege exec level 7 clear line
```

Risultati utente

I risultati seguenti si applicano agli utenti nelle configurazioni server riportate di seguito.

- **Utente uno**L'utente passerà l'autorizzazione Web se l'URL viene immesso come http://#.#.#.#.Dopo aver eseguito Telnet sul router, l'utente può eseguire tutti i comandi dopo l'autenticazione di accesso.L'utente sarà in modalità abilitazione dopo l'accesso (il **privilegio**

show sarà 15).

- **Utente tre**L'utente non riuscirà a ottenere l'autorizzazione Web perché non dispone di un livello di privilegio.Dopo aver eseguito Telnet sul router, l'utente può eseguire tutti i comandi dopo l'autenticazione di accesso.L'utente sarà in modalità non abilitazione dopo l'accesso (il **privilegio show** sarà 1).
- **Utente quattro**L'utente passerà l'autorizzazione Web se l'URL viene immesso come http://#.#.#.#/level/7/exec.Verranno visualizzati i comandi di livello 1 più il comando **clear line di** livello 7.Dopo aver eseguito Telnet sul router, l'utente può eseguire tutti i comandi dopo l'autenticazione di accesso.L'utente sarà al livello di privilegio 7 dopo l'accesso (**il privilegio show** sarà 7)

Configurazione RADIUS su server che supporta coppie AV Cisco

```
one Password= "one"
Service-Type = Shell-User
cisco-avpair = "shell:priv-lvl=15"

three Password = "three"
Service-Type = Login-User

four Password= "four"
Service-Type = Login-User
cisco-avpair = "shell:priv-lvl=7"
```

Configurazione server Cisco Secure ACS per UNIX

```
# ./ViewProfile -p 9900 -u one
User Profile Information
user = one{
profile_id = 31
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="one"
}
reply_attributes= {
6=6
}
}
}
# ./ViewProfile -p 9900 -u three
User Profile Information
user = three{
profile_id = 32
set server current-failed-logins = 0
profile_cycle = 3
radius=Cisco {
check_items= {
2="three"
}
reply_attributes= {
6=1
}
}
}
```

```
# ./ViewProfile -p 9900 -u four
User Profile Information
user = four{
profile_id = 33
profile_cycle = 1
radius=Cisco {
check_items= {
2="four"
}
reply_attributes= {
6=1
9,1="shell:priv-lvl=7"
}
}
}
```

Configurazione Cisco Secure ACS per Windows Server

- Utente = uno, tipo di servizio (attributo 6) = amministrativo
- Utente = tre, tipo di servizio (attributo 6) = accesso
- User = four, service type (attribute 6) = login, controllare la casella Cisco AV-pair e immettere shell:priv-lvl=7

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Comandi per la risoluzione dei problemi

I comandi seguenti sono utili per il debug dell'autenticazione HTTP. Vengono emessi sul router.

Nota: prima di usare i comandi di **debug**, consultare le informazioni importanti sui comandi di debug.

- **terminal monitor**: visualizza l'output del comando **debug** e i messaggi di errore del terminale e della sessione correnti.
- **debug aaa authentication**: visualizza le informazioni sull'autenticazione AAA/TACACS+.
- **debug aaa authorization**: visualizza le informazioni sull'autorizzazione AAA/TACACS+.
- **debug radius**: visualizza informazioni di debug dettagliate associate a RADIUS.
- **debug tacacs**: visualizza le informazioni associate a TACACS.
- **debug ip http authentication**: utilizzare questo comando per risolvere i problemi di autenticazione HTTP. Visualizza il metodo di autenticazione tentato dal router e i messaggi di stato specifici dell'autenticazione.

Informazioni correlate

- Pagina di supporto per il software Cisco TACACS+ Access
- Pagina di supporto RADIUS
- Pagina di supporto di Cisco Secure ACS per Windows
- Pagina di supporto di Cisco Secure ACS per UNIX
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems